Information Governance Policy

Document Control

1.1	**Document Author**	**Information Governance Manager**
1.2	**Status**	**Corporate Policy and Procedure**
1.3	**Version**	**Version 4**
1.4	**Approval Body**	**Document Review Group November 2011**
1.5	**Issue Date**	**January 2009**
1.6	**Effective Date**	**November 2011**
1.7	**Review Frequency**	**Three Yearly**
1.8	**Review Process and personnel**	**Document Review Group**
1.9	**Sign Off**	**Chair of Document Review Group**

Executive Summary

This document describes the Trust Policy for the maintenance of a robust Information Governance framework that will enable the effective management and protection of organisational and personal information held by the Trust, in accordance with the Trust strategy for Information Governance.

The Policy will set out the approach that the Trust will adopt to ensure that information, in all its different formats (i.e. paper or electronic), is managed in accordance with the law and national standards. The Policy will cover the overlapping areas of Data Protection compliance, Information Security (ISO27002 standard), Data Quality, Freedom of Information and Confidentiality (with regard to 'common law').

The purpose of this document is to provide the Trust with assurance that all aspects of Information Governance are being controlled through the utilisation of appropriate Policy.

CONTENTS

1 Introduction

1.1 Background

This document describes the Trust Policy for the maintenance of a robust Information Governance framework that will enable the effective management and protection of organisational and personal information held by the Trust, in accordance with the Trust strategy for Information Governance.

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

The Policy will set out the approach that the Trust will adopt to ensure that information, in all its different formats (i.e. paper or electronic), is managed in accordance with the law and national standards. The Policy will cover the overlapping areas of Data Protection compliance, Information Security (ISO27002 standard), Data Quality, Freedom of Information and Confidentiality (with regard to 'common law').

1.2 Purpose

The purpose of this document is to provide the Trust with assurance that all aspects of Information Governance are being controlled through the utilisation of appropriate Policy and in conformance with Version 8 of the IG Toolkit.

1.3 Responsibilities

The Trust has appointed an Information Governance Action Group that is responsible for developing and encouraging good information management practice amongst all members of the Trust. This group reports to the Safety and Quality Governance Committee.

The Trust has appointed an Information Governance Manager who is responsible for developing, facilitating and coordinating the implementation of the Trust's Information Governance framework to ensure that information assets are managed securely, and of high quality and integrity.

All staff members of the Trust are required to be aware of their obligations for ensuring that the governance of all items of information are managed in accordance with all current Trust Policy.

1.4 Monitoring and Review

All Trust staff are responsible for monitoring their personal compliance with the contents of this Policy. Departmental managers and supervisors should monitor compliance by their staff on a regular basis.

Adherence to this Policy will be monitored by the Information Governance Manager and reported to the Information Governance Action Group.

This document will normally be reviewed on a three yearly cycle and will be approved by the appropriate Board committee.

1.5 Related Documents

The following documents have an impact on this document, and have been consulted in the preparation of this paper:

- Access to Health Records Policy
- Adverse Events Policy
- Cancer Patients Information Sharing Protocol (Norfolk & Norwich University Hospital)
- Clinical Best Practice Strategy
- Computer Systems Access Control Policy
- Corporate Induction Policy
- Data Confidentiality – Keeping a clear Desk and Screen
- Data Protection Policy
- Data Quality Policy
- Data Transfers and Removable Media Policy
- Email Use Policy
- Freedom of Information Policy
- Governance Policy
- Health Records Management Policy
- IT Security Policy
- Information Governance Toolkit Website (provided by CfH)
- Information Risk Management Policy
- Internet Use Policy
- Norfolk NHS & Social Care Agreement (Protocol for Sharing of Personal Information)
- Patient Confidentiality Policy
- Patient Reception Process
- Procedural Documentation Development Policy
- Records Management: NHS Code of Practice Parts 1 and 2
- Registration Authority Smartcard Policy
- Risk Management Policy
- Signature Book Maintenance Policy
- Why a Patient's NHS Number is Important

1.6 Glossary

The following terms and abbreviations have been used within this document:

Term	Definition
BCM	Business Continuity Management
BT	British Telecommunications PLC
CDS	Commissioning Data Set
CfH	Connecting for Health
DPA	Data Protection Act
FOI	Freedom of Information
HES	Hospital Episode Statistics
ID	Identification
IG	Information Governance
IGAG	Information Governance Action Group
iPM PAS	NPfIT Patient Administration System
ISO	Information Security Officer
IT	Information Technology
JPUH	James Paget University Hospitals NHS Foundation Trust

NPfIT	National Programme for IT
PAS	Patient Administration System
PDS	Personal Demographic Service
SAR	Subject Access Request
PMO	Programme Management Office
SIRO	Senior Information Risk Officer
SLA	Service Level Agreement
SUS	Secondary Uses Service
TIG	Trust Investment Group
UPS	Uninterrupted Power Supply

1.7 Reader Panel

The following formed the Reader Panel that reviewed this document:

Post Title
Medical Director
Director of Finance & Performance
Head of IT
Deputy Director of Performance

1.8 Distribution Control

Printed copies of this document should be considered out of date. The most up to date version is available from the Trust Intranet.

2 Information Governance Scope

Information Governance is a systematic approach to ensuring that all aspects of the processing of personal and sensitive information (both paper and electronic), meet prescribed standards. It aims to ensure that performance is subject to continuous improvement. The Information Governance framework has four dimensions:

- Management : structures, policies, procedures, etc.
- Systems : access controls, application security, validation, etc.
- Processes : protocols, records management, data quality, etc.
- People : education, training, development, guidance, etc.

This section describes the mechanisms and controls that the Trust will employ to manage Information Governance and to ensure that all aspects are being appropriately addressed.

2.1 Information Governance Management

2.1.1 Management Structure and Governance Framework

The Trust's overall Governance arrangements are described in the Governance Policy (available on the Trust Intranet, under Policies & Guidelines, Corporate). The Terms of Reference for the responsible bodies at each level of Governance are held within the Trust's Risk Management Policy available on the Intranet (under Policies & Guidelines, Risk Management). Refer to this document for the Trust's committee structure and reporting lines.

Responsibility for Information Governance rests with the Information Governance Action Group (IGAG). IGAG reports to the Trust's Safety and Quality Governance Committee. The Safety and Quality Governance Committee have delegated authority from the Board of Directors for Governance matters. The IGAG will be chaired by the Trust's Medical Director and a number of other Board members and various Heads of Department will sit on the group. The IGAG will meet formally on a regular basis.

2.1.2 Procedural Documentation

Procedural documentation covering all Strategy, Policy and Procedure documents will be managed through the Trust's Document Review Group. This is primarily a logical group that meets on a quarterly basis to ensure that due process is being followed.

This Group has a published Terms of Reference and its activity will be directed by the Trust's Procedural Document Development Policy. All Trust Strategy and Policy documents will be published on the Trust Intranet.

The Group will be chaired by the Assistant Director of Governance, Safety & Compliance, who will hold the Terms of Reference for the forum.

2.1.3 Contract Management

Contracts with suppliers are drawn up on a Departmental basis, using an approved format from the Trust's Legal Department. This includes the 'NHS conditions of contract for the supply of services' template (dated July 2005), which is centrally sourced and fully adheres to IG requirements.

A Register of all Third Party contracts has been created by the Trust and ownership for the maintenance of this register allocated rests within the Finance Department.

Contracts and standard Terms and Conditions for staff are developed by the Trust's Human Resources Department; these include agreement to maintain confidentiality of information. These are reviewed periodically and when changes to best practice relating to Information Governance matters are published. Responsibility for this review rests with the Director of HR.

2.1.4 Staff Training and Awareness

The Department of Health have approved the Trust's staff Induction Training material as suitable to be used in place of the nationally provided e-learning packages for Information Governance.

Attendance at Staff Induction training is mandatory for all new staff. The Trust's Corporate Induction Policy (available on Trust Intranet under Policies & Guidelines, Human Resources) describes the content of the mandatory Corporate Induction training program, which covers all aspects of the Information Governance framework.

The Trust is currently developing an approach to enhanced Information Governance training for existing staff and this forms part of the current Information Governance Strategy and the current IG Improvement Plan.

2.1 Confidentiality and Data Quality Assurance

2.2.1 Confidentiality and Data Protection

The Trust's confidentiality and consent arrangements are described in the Patient Confidentiality Policy. Good practice is also documented in the 'Data Confidentiality – Keeping a clear desk and screen' and 'Patient Reception Process' guidance documents.

Adherence to this Policy will be monitored by the Caldicott Guardian and the Information Governance Action Group by virtue of normal business activities of its membership, and the Patient Advice and Liaison Service will report patient issues and experience to the Information Governance Action Group.

The Trust's Data Protection Act arrangements are described in the Data Protection Act Policy.

The Information Governance Manager fulfils the role of Data Protection Officer for the Trust. This post sits within the Trust's Information Services Department.

Adherence to this Policy will be monitored by the Information Governance Manager and the Information Governance Action Group.

2.2.2 Patient Access to their Health Care Files

The processes for Subject Access Requests (SAR's) from individuals to the Trust and for patient access to the contents of their Health Care Files are described in the Trust's 'Access to Health Records Policy and its supplements. There is also further information in the 'Health Records Management Policy'.

Management of these processes will be carried out by the Trust's Health Records Service Manager. This post sits with the Trust's Information Services Department.

2.2.3 Systems Access

The Trust's Information Security Officer is the Head of IT, and this role has responsibility for ensuring that the access controls in place for all the Trust's key systems meet the requirements of information security standards.

Each computer system will have an appropriately empowered Systems Administrator (or Access Co-ordinator) who will provide and manage user access to the system on guidance from appropriate Line Managers.

The Trust's access arrangements to IT systems are described in the Computer Systems Access Control Policy.

Adherence to this Policy will be monitored the appropriate System Administrator, and reports of non-compliance will be produced as appropriate to Line Managers and the Trust's Information Security Officer. These will be addressed to the Information Governance Action Group as appropriate.

2.2.4 Protocols Governing the Sharing of Patient-Identifiable Data

The Trust is a signatory to the Norfolk NHS & Social Care Agreement called 'Protocol for Sharing of Personal Information', and this is applied equally for Suffolk based patients.

The Trust also shares a 'Cancer Patients Information Sharing Protocol' with the Norfolk & Norwich University Hospital (available from Head of Information Services).

The Trust has developed a register of Data Sharing Partners used by the organisation and this is published on the Trust's intranet, under the Information Governance section.

2.2.5 Data Protection

The Trust's Data Protection arrangements are described in the Data Protection Act Policy.

The Information Governance Manager fulfils the role of Data Protection Officer for the Trust. This post sits within the Trust's Information Services Department.

2.2.6 Controls for New Processes, Software and Hardware

Any requirement for a new system will be put through the Trust process for authorisation (the 'Trust Investment Group'), which will consider the financial, business and security implications.

The Trust is currently developing a formal Trust Investment Group Policy that will be administered by the Audit Committee.

The Programme Management Office (PMO) for the Trust's IT Department have developed formal processes to ensure that Information Governance requirements are considered for all new or revised IT solutions and will consult with the Information Governance Manager during specification and procurement.

2.3 Information Security Assurance

2.3.1 Information Security Risk Assessment

The Trust's Information Security Risk arrangements are described in the Information Security Risk Management Policy.

The Senior Information Risk Officer (SIRO) for the Trust in nominated as the Director of Finance and Performance, who is a member of the Trust Board.

The SIRO will be the advocate for information risk on the Board and ensure that identified information security threats are followed up and incidents managed. They will also ensure that the Board and the Accountable Officer are kept up to date on all information risk issues. This role also maintains ownership of the Information Risk Policy and risk assessment process.

Information risks will be reported via the Trust's electronic incident management systems (Safeguard). This is available to all staff via the Trust intranet.

2.3.2 Information Asset Ownership

The Trust's Information Asset Management arrangements are described in the Information Security Risk Management Policy.

The Information Governance Manager will administer the Trust's Information Asset Register. This includes details of risk assessments that have been carried out.

For physical assets (Computer equipment, communications equipment, etc), where ownership of an item resides with the Trust, then the IT Department will be responsible for implementing and maintaining an asset register. Where physical assets are purchased separately by a Department then they are responsible for keeping a local asset register up to date.

2.3.3 Access Controls

Access to information should be controlled on the basis of business need, security requirements and the user's role in the operation of the Trust. Controlling access to information is one of the key elements of organisational compliance with legislation such as the Data Protection Act. Access control works on two levels; the physical access control (access to buildings and facilities) and the system access control.

The Trust's arrangements for system access control are described in the Trust's Computer Systems Access Control Policy.

The Trust's arrangements for Registration Authority (RA) access control for national systems are described in the Trust's Registration Authority Smart Card.

The Trust's arrangements for physical access control are described in the Trust's Security Policy, Procedures and Guidance document, particularly Appendix 2.

2.3.4 Operating Systems

The Trust's corporate computer systems will provide a number of standard Microsoft tools to Users and acts as a gateway for Users who use e-mail or need to access the Internet.

Access to the Trust's corporate computer systems will be controlled through a formal request and registration process at the start of the User's employment with the Trust. The Head of IT will manage this. Access to Operating system software will be limited to the staff in the Trust's IT Department.

The Trust's arrangements for Operating System access control are described in the Trust's Computer Systems Access Control Policy.

2.3.5 Application Systems

Each computer system will have an appropriately empowered Systems Administrator (or Access Co-ordinator) who will provide and manage user access to the system on guidance from appropriate Line Managers.

The Trust's arrangements for Application System access control are described in the Trust's Computer Systems Access Control Policy.

2.3.6 Digital Information Security

The secure exchange of information by electronic means with any other organisation is paramount to the Trust. This is embodied in a number of policies and guidance documents made available to all members of the Trust (see Trust Email Policy, Internet Use Policy and the Data Transfer and Removable Media Policy).

The Trust has implemented effective encryption of USB devices, Laptops, PACS images, Secure CD/DVD destruction and limited CD/DVD creation ability. The Trust has ongoing Projects to implement the following security measures in the future. Completion of these will be managed by IGAG:

- PDA encryption

IT tools for the automated monitoring of email traffic content from Trust email accounts looks specifically for information that relates to patients (e.g. Hospital number) and will flag any such emails to the IT Team for recording the Safeguard system.

2.3.7 Availability of Key Systems

The Trust's Disaster Recovery Procedures cover all locally maintained hardware and systems, and are maintained by the Head of IT. These include details of backup and recovery processes for all IT systems.

All local servers are maintained in secure rooms with full environmental protection in place and access will be strictly controlled by the Head of IT. All servers have dual components wherever this is technically possible. All servers have dial-in components where this is technically possible and costs permit

The Trust's Patient Administration System (iPM PAS) is provided by the local NPfIT supplier under contract to the Department of Health, which provides an SLA for service availability, however this is outside of the control of the Trust.

The Trust has local processes in place for the management of patients in the event of any key system unavailability.

2.3.8 Detection, Isolation and Removal of Malicious or Unauthorised Software

The Trust operates virus and intruder protection at a server and individual PC level, using different products with independent code repositories to ensure new modes of attack are captured at both levels and as quickly as the protection becomes available commercially. Updates are regularly sourced from the software suppliers in accordance with best practice.

The ability to install new software on Trust equipment will be restricted to the IT Department, to ensure that appropriate licensing and adequate protection of the Trust infrastructure is maintained at all times.

2.3.9 Secure Communication Networks

Responsibility for the Trust's IT Network resides within the IT Department, under a 'Engineering Manager' post. This post will be responsible for implementation of appropriate controls.

The Trust's network and technical environment include multiple levels of Firewalls, software monitoring of the network and all activity going through it. There will also be controlled access to the Internet which will be fully monitored. This will be in accordance with the current industry standards.

The Trust has N3 connection provided by CfH for all NPfIT systems. This is monitored and maintained by BT.

2.3.10 Secure Mobile Computing and Remote Access

Trust policy is that remote access is only provided to individuals who are able to justify a business reason for such access. Access will be provided by the IT Department through the use of secure token technology.

The Trust's arrangements for Remote Access and Mobile Computing are described in the Trust's Remote Access Policy (available from the IT Department).

2.3.11 Pseudonymisation/Anonymisation Techniques

Procedures for the pseudonymisation or anonymisation of person identifiable data where it is required for secondary uses are owned by the Trust's Information Services Department.

2.4 Clinical Information Assurance

2.4.1 Information Quality and Records Management

The Trust's Information Governance Action Group has responsibility for information quality and records management. This is reflected in its published Terms of Reference. The Director of Finance and Performance takes responsibility for Corporate Records, the Director of Workforce and Estates for Staff Records and the Health Records Service Manager for patient Health Care Files.

2.4.2 NHS Number Utilisation

The Trust maintains a local Hospital Number for all patients as the primary reference for patients internally. All Trust patients are registered into the Trust's Patient

Administration System (iPM PAS). As part of this process, the patient record is checked against the national Patient Demographic Service (PDS) to identify the NHS number for that patient.

The NHS number for the patient will be included in all patient documentation and correspondence.

The Trust's approach to the use on NHS numbers is described in the guidance document 'Why a Patient's NHS Number is Important'.

2.4.3 Clinical Record Keeping Standards

The Trust will carry out regular audits of clinical record keeping standards. Audits are carried out to support National Institute for Health and Clinical Excellence (NICE), CNST, Healthcare Standards and National Service Frameworks (NSF) audit requirements. Audits will also include validation of patient information across electronic systems.

Details of the Audit schedule, tools, records and reports for these audits are maintained by the Trust's Clinical Governance & Effectiveness Manager).

Audits are carried out either by the Audit Department or by Speciality staff themselves (with or without support from the Audit Department)

The Clinical Audit and Effectiveness Steering Group will be responsible for the review of compliance and monitoring of all national best practice guidance, and reports to the Clinical and Medical Review Group.

This activity is supported by the Trust's Signature Book Maintenance Policy and Clinical Best Practice Strategy.

2.4.4 Standard Health Care File Construction

All staff that will be required to manage patient Health Care Files as part of their role will be trained in the construction and use of these, by The Trust's Health Records Department, before they are provided with access to the iPM PAS system by the IT Department. The Health Records Manager will maintain a register of such training.

The construction of the Health Care File is detailed in the Trust's Health Records Management Policy. Adherence to this Policy will be managed by the Health Records Management Committee, which will report its finding to the Information Governance Action Group. Regular reports will also include the availability of Health Care Files and the actions taken to trace missing HCF's.

2.5 Secondary Uses Assurance

2.5.1 Use of NHS Standard Definitions

The Trust has implemented a number of NPfIT applications, including the pivotal iPM Patient Administration System. As these applications are centrally developed and managed, these applications fully adhere to NHS standard definitions, as prescribed by the NHS Data Dictionary.

The use of NHS standard definitions will be a standard requirement for the IT Department when systems are evaluated or developed. All Key Systems have drop down menus to ensure staff are only selecting authorised data values.

All Trust activity reporting is made through the NHS SUS system. This validates the information supplied against the National Standards. HES also validate the information supplied via SUS and provide reports that the Trust uses to verify that all appropriate National Standards are being used consistently.

Changes to any standards or definitions are communicated nationally via electronic 'Information Standard Bulletins'. Information Services have a process in place for receiving and reviewing these ISB's and for communicating information from these to the Trust as appropriate.

2.5.3 Local and National Benchmarking

The local procedures for the Trust's Information Services Department include details of regular data collection and quality checks that are carried out. These include data quality checks using both local and national sources. Key Data items will be validated by data quality checks carried out by the Information Services Department when Trust performance data is submitted to SUS.

Processes surrounding the reconciliation of Trust activity data submitted to SUS with the PCT include the investigation and resolution of any perceived data quality issues.

The 'Dr Foster' application will be used by the Trust to compare data trends internally and against other Acute Trusts.

2.5.4 Clinical Coding Quality Audits

The Trust uses external staff who are registered on the national list of approved clinical coding auditors to perform a clinical coding audit based on the requirements and standards within the 'Data Quality Audit Framework for Coded Clinical Data'. This will normally performed on an Annual basis. The Trust will use the results of this external audit to review and revise its Clinical Coding processes. The results of this audit are circulated to IGAG for awareness and discussion.

The Trust is not currently required to undergo an annual external clinical coding audits commissioned by the Audit Commission.

2.5.5 Patient Record Keeping Standards

The Trust will carry out regular audits of record keeping standards for Patient information.

The Trust's Clinical Governance & Effectiveness Department have developed a 'Documentation Audit Data Collection Form' to manage this assessment. This forms a procedural mechanism for checking the quality of data in the iPM PAS system against the Health Care File for the patient.

Details of the Audit schedule, tools, records and reports for these audits are maintained by the Trust's Clinical Governance & Effectiveness Manager).

2.5.6 IG Completeness and Validity check for Data

The Information Governance Assessment toolkit includes a requirement for the Trust to demonstrate the completeness and validity of data being used for submission of Commissioning Data Set (CDS) files to SUS. This is completed by a mathematical representation of data conformance and the Trust must demonstrate the reconciliation between the SUS return and the data source (iPM PAS).

This annual exercise will be carried out by the Information Services Department in accordance with the guidance in the Information Governance Assessment Toolkit.

2.5.7 Formal Training for Staff in the Operation of Key Systems

The Trust has developed formal training programmes for the operation of each of the Key Systems in use. The System Owner for each of the Key systems will be responsible for ensuring that each member of staff is appropriately trained to use that system. Details for each of these training programmes are held by the Head of IT.

Users will not be granted access to these systems until appropriate training has been completed and documented.

The Corporate Training database is set up to record attendance of individual staff on these training programmes and the System Owner for each system will be responsible for ensuring that the database is updated for each member of staff completing the appropriate training.

For the Trust's NPfIT systems, the RA Manager will not permit the processing of RA02 forms to change a User's access rights until the completion of the appropriate training has been verified by the IT Training Department.

2.6 Corporate Information Assurance

2.6.1 Management of Corporate Records

All Policy and Guidance documents will be stored on the Trust Intranet once they have been approved by the appropriate body. The Trust's corporate document creation arrangements are described in the Procedural Documentation Development Policy.

The Trust Intranet is managed on servers that are subject to full and regular backup regimes, that would enable full recovery of any lost record as required. All other Trust documents and files are stored on servers that are subject to full and regular backup regimes, that would enable full recovery of any lost record as required. Directory structures on these servers are left to the discretion of the User.

2.6.2 Freedom of Information Act 2000

The Trust Web site has a FOI section that provides both email and white mail contact details for all FOI requests to the Trust. Any requests for information received by the Trust are to be directed to the Head of Risk Management and Governance who will be responsible for evaluating the request and coordinating the Trust response.

FOI requests will be reviewed and performance against the Policy assessed as part of Information Governance Action Group meeting agenda.

The Trust's FOI arrangements are described in the Freedom of Information Policy (available on the Trust Intranet, under Policies & Guidelines, Corporate).

3 Information Governance Conformance

3.1 Measurement

The Trust will measure its achievement of Information Governance requirements on an annual basis by the completion of the on-line CfH Information Governance Toolkit.

Details of the Toolkit can be found at the following website:

https://nww.igt.connectingforhealth.nhs.uk/

The Information Governance Action Group will deliver an annual report of the Trust's achievement against this Toolkit to the Safety and Quality Governance Committee.

3.2 Progression

The Trust will seek to achieve a year on year improvement of its Information Governance conformance by the development of an annual Improvement Plan.

This Improvement Plan will be developed by the Information Governance Action Group and delivered to the Safety and Quality Governance Committee for approval.

Progress against this Improvement Plan will be managed by the Information Governance Action Group during the course of each year.

Appendix A Equality Impact Assessment

Policy or function being assessed: INFORMATION GOVERNANCE POLICY Department/Service: CORPORATE

Assessment completed by: RUSSELL CRAWFORD Date of assessment: 31 JANUARY 2010

1.	Describe the aim, objective and purpose of this policy or function.		This document describes the Trust Policy for the maintenance of a robust Information Governance framework that will enable the effective management and protection of organisational and personal information held by the Trust, in accordance with the Trust strategy for Information Governance.	
2i.	Who is intended to benefit from the policy?		**Staff** ☐ **Patients** ☐ **Public** ☐ **Organisation** ☑	
2ii	How are they likely to benefit?		Appropriate policies, procedures and management accountability and structures are in place to provide a robust governance framework for information management.	
2iii	What outcomes are wanted from this policy?		Improving performance against scoring in the CfH IG Toolkit	
For Questions 3-8 below, please specify whether the policy/function does or could have an impact in relation to each of the six equality strand headings:				
3.	Are there concerns that the policy does or could have a detrimental impact on people due to their **race/ethnicity?**		**N**	If yes, what evidence do you have of this? Eg. Complaints/Feedback/Research/Data
4.	Are there concerns that the policy does or could have a detrimental impact on people due to their **gender?**		**N**	If yes, what evidence do you have of this? Eg. Complaints/Feedback/Research/Data
5.	Are there concerns that the policy does or could have a detrimental impact on people due to their **disability?**		**N**	If yes, what evidence do you have of this? Eg. Complaints/Feedback/Research/Data

6.	Are there concerns that the policy does or could have a detrimental impact on people due to their **sexual orientation and/or transgender?**		**N**	If yes, what evidence do you have of this? Eg. Complaints/Feedback/Research/Data
7.	Are there concerns that the policy does or could have a detrimental impact on people due to their **age?**		**N**	If yes, what evidence do you have of this? Eg. Complaints/Feedback/Research/Data
8.	Are there concerns that the policy does or could have a detrimental impact on people due to their **religious belief?**		**N**	If yes, what evidence do you have of this? Eg. Complaints/Feedback/Research/Data
9.	Could the impact identified in Q.3-8 above, amount to there being the potential for a disadvantage and/or detrimental impact in this policy?		**N**	
10.	Can this detrimental impact on one or more of the above groups be justified on the grounds of promoting equality of opportunity for another group? Or for any other reason? Eg. providing specific training to a particular group.		**N**	*Where the detrimental impact is unlawful, the policy or the element of it that is unlawful must be changed or abandoned. If a detrimental impact is unavoidable, then it must be justified, as outlined in the question above.*

11.	**Specific Issues Identified**	
	Please list the specific issues that have been identified as being discriminatory/promoting detrimental treatment	Page/paragraph/section of policy that issue relates to
	1. Not applicable	**1.**
	2. Not applicable	**2**
	3. Not applicable	**3**
12.	**Proposals**	
	How could the identified detrimental impact be minimised or eradicated?	**Not applicable**

	If such changes were made, would this have repercussions/negative effects on other groups as detailed in Q. 3-8?		**N**
13.	Given this Equality Impact Assessment, does the policy need to be reconsidered/redrafted?		**N**
14.	**Policy/Practice Implementation**		
	Upon consideration of the information gathered within the equality impact assessment, the Director/Head of Service agrees that the policy/practice should be adopted by the Trust. Please print: **Name of Director/Head of Service: MARK MADDEN Title: DIRECTOR OF FINANCE & PERFORMANCE** **Date: 31 JANUARY 2011** **Name of Policy Author: RUSSELL CRAWFORD Title: INFORMATION GOVERNANCE MANAGER** **Date: 31 JANUARY 2011** (A paper copy of the EIA which has been signed is available on request).		
15.	**Proposed Date for Policy/Practice Review**		
	Please detail the date for policy review (usually three yearly): JANUARY 2014		
16.	**Explain how you plan to publish the result of the assessment?** *(Completed E.I.A's must be published on the Equality pages of the Trust's website).*		
	Standard Trust process		
17.	**The Trust Values**		
	In addition to the Equality and Diversity considerations detailed above, I can confirm that the four core Trust Values are embedded in all policies and procedures.		

	They are that all staff intend to do their best by: Putting patients first, and they will: Provide the best possible care in a safe clean and friendly environment, Treat everybody with courtesy and respect, Act appropriately with everyone. Aiming to get it right, and they will: Commit to their own personal development, Understand theirs and others roles and responsibilities, Contribute to the development of services Recognising that everyone counts, and they will: Value the contribution and skills of others, Treat everyone fairly, Support the development of colleagues. Doing everything openly and honestly, and they will: Be clear about what they are trying to achieve, Share information appropriately and effectively, Admit to and learn from mistakes. I confirm that this policy does not conflict with these values ☑